GDPR compliance and Data Security Policy at Netkin

Last update: October 22nd, 2022

This document explains how Netkin enforces GDPR compliance, and which measures are in place to ensure the security of your and your participants' personal data.

What is GDPR ?

GDPR stands for "General Data Protection Regulation", a new European Union level regulation coming in effect on 25 May, 2018.

This regulation is designed to **harmonize data privacy laws across Europe, enhance protection of EU citizens' personal data, and improve the way organizations approach this data.** It's very important to know about the changes, because non-compliance can mean heavy fines for businesses and organizations.

As an event organizer, how does this affect me?

Probably the biggest change is the extended jurisdiction of the GDPR. Starting 25 May 2018 the rules for data protection will apply to all companies processing personal data of EU citizens, regardless of the company's location.

The GDPR will also apply to the processing of personal data for EU citizens, where the activities relate to: offering goods or services (free or paid) to EU citizens, as well as monitoring behaviour within the EU. Non-EU businesses that process EU citizens data are required to appoint a representative in the EU.

So yes, as long as some of your participants might be EU citizens, you are concerned, and your processes and tools must be GDPR-compliant.

What are the risks of non-compliance ?

If your business or organization is found to be in breach of GDPR, you face a substantial fine. The maximum can be up to 4% of your annual global turnover or €20 Million, whichever is higher. Fines are imposed for infringements like:

- insufficient customer consent to process data;
- violations of the Privacy by Design concept;
- failure to implement sufficient data protection measures;
- failure to inform the competent authority and data subjects of a breach.

What are my obligations and what are Netkin's obligations ?

The GDPR defines two roles in the process of managing your participants' data : The Data Controller, and the Data Processors.

The Data Controller (You and/or your client, as an event organizer)

The Data Controller refers to the person or company who decides what information is collected, for what purpose, and how it is processed. According to EU law, the Data Controller's obligations include, but are not limited to:

- providing clear information to your participants about the personal data you collect and for what purpose ;
- obtaining clear consent of the participant that they agree to provide their personal data for that purpose ;
- Provide a simple way for the participant to request to erase and/or stop the release of the data, and, potentially, for third-party processors to stop processing this personal data and for the data to be returned to the participant in a readable format (for example Excel)

Netkin has enforced since May 2018 that all registration websites have a mandatory checkbox on the first registration step with a standardized text covering these 3 obligations. We strongly advise you to double check this text with your internal legal service, or the legal service of your client, to ensure it is compliant with country or company policies.

The Data Controller's obligations also include :

- to keep and process only the data absolutely necessary for the completion of its tasks (data minimisation). Additionally, to limit and control the data processors' access to such personal data ;
- to protect personal data against accidental loss, unauthorized access, or unlawful processing ;
    - **Netkin ensures this protection at the platform level (see below), but the security of your mailbox, computer, software, etc. is your responsibility ;**

- to establish written agreements with data processors - who have access to customer data under your authority - that require them to act only on your instructions and ensure that they comply with all data protection requirements ;
- to inform participants within 72 hours of a data breach - or awareness of one ; to ensure that all data processors meet the requirements (see below).

Data Processors (Netkin and our hosting company OVH, and your other subcontractors)

A Data Processor is any person or company that processes personal data for the Data Controller, such as the registration platform, event app, data analytics, hosting or storage services, etc.

IMPORTANT : If you export data from Netkin platform (for example as Excel file) you are a data processor as well, and obligations of Data Processors also apply to you and all your subcontractors that might have access to this exported data (freelance managing participant registration, or badge printing subcontractor for example).

The requirements for The Data Processors include, but are not limited to :

- process data reasonably, lawfully, and for legitimate purposes ;
- implement all appropriate security measures to protect the personal data ;
- informing the controller immediately of any data breaches ;
- keep internal records of all data processing activities ;
- enforce privacy by design : this means the inclusion of data protection from the onset of the designing of systems, rather than an addition. Specifically, you have to implement appropriate technical and organizational measures to meet the requirements of the new regulations and protect the rights of data subjects.

Netkin implemented appropriate measures to be fully compliant with these requirements. (See bellow)

Netkin’s Data Security Policy **Privacy by Design**

Since the beginning, **Netkin’s solution was built on the principle of Privacy By Design**

- Each event has its own platform (instance of our solution), fully isolated on our dedicated servers hosted at OVH (we do not use a public cloud), with its own private database.
- Each event instance has no way to communicate with other event platforms, despite their presence on the same physical server: CloudLinux's "Cage FileSystem" technology isolates each instance on the server in an independent file system, preventing it from seeing the existence of other instances on the same server.

- Our automated deployment system cannot access the event instances after deployment, it can only send them configuration or backup instructions, not giving access to the data. Even in case of backup, the instance itself encrypts the backup in AES256-cbc, and sends the decryption key to a "secure safe" located on another dedicated server that is not accessible from the outside. This key is different for each backup and for each instance.
- In an event instance, privileged users (administrators in charge of participant registration) have fully audited access control.
- All privileged users must authenticate by default using the 2FA (automatic login link with strong hash confirmation code + SMS).
- In an event instance, a participant cannot access other participants' data, except in the who's who, where you can choose which fields to display. By default, email, phone number or other sensitive data is not included, in which case this data is not even downloaded to the participants' machines. Only privileged users that you (the client's primary administrator) appoint can access it.
- No Netkin staff can access your event platform administration without your explicit permission
- No Netkin technical staff may access your Event Platform's source code or data without the approval of a Netkin associate.

Automated pentests

- Each of our new releases is scanned using the latest version of Acunetix, directly on the production server, before it is released
- Upon request, we can perform such a security scan on your event instance once it is ready, as an anonymous user and as a logged-in participant only (the security scan as a privileged user will modify the content of your platform). Due to our competitive pricing, this additional scan will be charged at a flat rate, and a scan report will be provided to you.

Human pentests

Each new version of our solution is human pentested before its release by Lexfo, and continuously monitored by their Ambionics solution. The result of the last pentest is available on demand.

In parallel, several times a year, our customers request to perform penetration tests or live security scans on an instance. This can only be done within the following scope: by performing tests (of any type) on one of our instances and/or server, you fully respect the restrictions mentioned below - you could be liable for any damage caused by not respecting these restrictions.

- No technical access to the server will be provided (this is strictly non-negotiable as our source code is not disclosed for security reasons).
- On your production instance, pentesting or scanning while logged in with a privileged (administrator) account is strictly prohibited as this could alter the site structure and/or content, and send unwanted emails. Privileged accounts have the ability to export all data anyway.
    - If you want to perform a pentest using a privileged account, you can ask us to create a clone of your instance, once dynamic contents are ready (registration form, interactivity pages, social feed, etc.)
- No testing that could alter data and/or quality of service is allowed because your target instance (cloned or not) will reside on a production server.
- No DDoS tests are allowed (our hosting provider OVH has a data center level DDoS protection).
- You are not allowed to export or disclose any data you may have access to during the test.

Security of storage and production servers

Data is hosted exclusively on dedicated OVH servers in France, located in OVH's main data centers in Roubaix (France), Gravelines (France) and Strasbourg (France).

- **Physical security measures for OVH datacenters:** https://www.ovh.com/fr/protection-donnees-personnelles/securite.xml
- **Front-end servers** (Apache 2.4, php 8.2): CloudLinux 7.x (hardened version of CentOS 7.x, specifically designed for instance-isolated web hosting), WHM / CPanel with CPHulk (brute force protection) and built-in firewall. No client database on this server.
    - Using CageFS technology (provided by CloudLinux), each instance runs in its own "caged" file system and cannot see files, data, processes of other instances, nor sensitive files of the server configuration. More information on https://cloudlinux.com/index.php/cagefs ;
    - None of our customers have administrative or technical access to the server (no FTP or MariaDB, CPanel, or shell access, etc.) ;
    - Fully automated updates and patches for CPanel and CloudLinux/CentOS, with a summary sent by email to CSO, and a monthly human check ;
    - ClamAV antivirus with automated daily scanning ;
    - DDOS protection by OVH ;
    - Apache 2.4 / PHP 8.2 ;
    - The Imunify360 solution is integrated into our servers to detect and block intrusion attempts (more information later in this document)
    - Administrative access to the server is all filtered via IP, only connection through our secure VPN is possible. (OpenVPN Access Cluster managed by us on dedicated OVH servers, with individual accounts, password rotation every night, daily mandatory 2FA OTP, and audit of all connections in OpenVPN) ;

    - Brute force protection on all server authentication mechanisms, and on the authentication mechanisms of each instance ;
    - Apache logs are analyzed daily in an automated way via Datadog, and weekly in a human way, in order to detect any security or performance anomaly.

- **Cluster of database servers (mariadb 10.6.x):**
    - CentOS 7.x, only port 3306 is allowed through the firewall, on private LAN (VRack by OVH), with data encryption on disk.
    - This cluster is not accessible from the Internet.
    - On the database servers, each instance has its own database, with credentials known only to that instance. Our instance management solution itself does not know these credentials.
    - The default credentials and accounts are either disabled or changed automatically during the provisioning of each server.

Backup Security

Backup process

- Each backup performed is encrypted with a random key. This key is itself encrypted with a key specific to the instance, then the result is sent by the instance being backed-up directly to a Netkin mailbox (hosted by gmail for business), to which only the 3 operational associates have access. The 2FA is activated on this mailbox, and its connection audit is activated.
- In parallel, the encrypted backup is uploaded to a dedicated OVH storage server, in a French datacenter different from those on which the instance is running.

Restoration process

- Restoring a backup can only be done by being connected to our instance manager, which is only accessible from our technical VPN (OpenVPN Access Cluster managed by us on dedicated OVH servers, with individual accounts, password rotation every night, daily mandatory 2FA OTP, and audit of all connections in OpenVPN) ;
- Only developers with more than 3 years of permanent employment have such a VPN account, created exclusively by the CTO.
- Restoring a backup also requires knowing the encrypted key of this specific backup, which the developer must ask to one of the 3 operational associates.
- Our automated instance manager can then decrypt the encrypted encryption key of the backup, using the key-encryption key, not known to developers. The hereby decrypted encryption key is of course not stored or logged.
- Any operation/access in our instance manager is logged without time limit.

Access to the backup storage server

- Since access to the backup storage server is not necessary for restoration, only the CTO (majority partner) and the deputy CTO (also a partner) can connect to it via SSH, accessible only from the IP address of our technical VPN (OpenVPN Access

Cluster managed by us on dedicated OVH servers, with individual accounts, password rotation every night, daily mandatory 2FA OTP, and audit of all connections in OpenVPN) ;
- If OVH accesses the storage server, it would in any case not have the decryption keys for the backups, and would not be able to know which backup file corresponds to which client, their name being a salted asymmetric hash sha512.
- Also, since the decryption key itself is encrypted, a collaboration between a malicious employee on both sides would not allow decrypting a backup.

Access to the source code of the instance manager

- Only the CTO (majority partner), and the deputy CTO (also partner) have the possibility to connect to it in SSH, by being connected to the technical VPN (firewall) beforehand.

Real-time automated monitoring and protection :

We use the Imunify360 solution in each of our production instances. This solution intervenes before each request is processed by the server (upstream of Apache), to protect each instance with various security modules, including :

- Real-time monitoring of logs and requests
- Pro-active defense against attacks via PHP (kill mode)
- WAF (Web Application Firewall), with the following rules enabled
    - OWASP ModSecurity Core Rule Set V3.0 (https://go.cpanel.net/modsecurityowasp)
    - Imunify360 ModSecurity Rules For Apache https://docs.imunify360.com/
- Each request that triggers one of these rules is blocked before reaching apache (403 response)
- When an IP (including behind a CDN or Cloudflare) is blocked at least 4 times in a row within 1 hour, it is added to the greylist:
    - This IP is blocked at the firewall level on any other port than 80 and 443
    - On port 443 and 80, this IP is submitted to a captcha to verify that it is not a bot.
    - If the captcha is presented at least 100 times, the IP is blacklisted from the server at the firewall level, and cannot connect on any port for 7 days.
- Complete list of features: https://www.imunify360.com/

Security Principles for Software Development

Each code contribution of our developers is reviewed by Netkin CTO/CSO, to check for performance bottlenecks and ensure that every piece of code follows OWASP guidelines (https://www.owasp.org/index.php/OWASP_Code_Review_Guide_Table_of_Contents), amongst which :

- Development, test and prod envs are on physically separate networks (OVH v-rack) and physically separate servers. We don’t use any customer’s data during our tests.

- Transport security:
    - https mandatory with fully trusted certificate, and HSTS
    - weak ciphers or protocols have been disabled
    - Qualys SSL Labs quality grade : A+
    - Report : https://www.ssllabs.com/ssltest/analyze.html?d=pentest.event.netkin.io&hideResults=on
- Password and authentication security : Authentication by password is forbidden by default, we use autologin links, which security is stronger since it does not involve a human element (the password). Besides, it avoids employees to put their corporate passwords by reflex. Autologin links work as follows:
    - Autologin links are using random token with very long verification hash : https://nameoftheventwebsite.com/trk/437-FDimZkGaIfmYdMDkimWT--nkwsid169-7a3505564affeec839987386ee0a41f0c08aeb2bb122b85d26e4d0a7fa4dde6e-c5d4156451-bfe7a71f3abc87ac28ecb051e2484b7c9dfa1ea917eb2921f69bda96f11b8c25
    - Unicity of every random string is enforced by storing their sha256 hash.
    - IP-based brute-force protection of 8 attempts, disabling the ability to authenticate for the IP during 30 minutes
    - Administrative access to the instance is reinforced by default using single-use two-factor authentication (Single use token link sent by email based on browser session, which has to be validated using single-use numerical code sent by SMS)
    - When a privileged user logs in from an unknown IP address, or from a new browser, all users with the user rights management privilege can be notified by email, with single-use link allowing immediate account locking
    - Authentication cookies and session cookies are HttpOnly and Secure. Our application stores a hashed representation of the cookie's value when it gets sent, and then compares the received cookie's value to ensure they are the same.
- Mixed Content :
    - All resources are loaded from domain name, no use of CDN
    - Cross Site Request Forgery (XSRF or CSRF) : Requests triggering data modification are only done through POST. Each POST request is validated with CSRF token. If missing or wrong, the request is blocked.
    - Cross Site Script Inclusion (XSSI) : All JSON requests are done through POST only
    - Clickjacking : header X-Frame-Options: SAMEORIGIN sent on each page
- 3rd Party Content : all resources are served from website server and domain name
- Input Validation
    - SQL Injection : All requests containing user input use parameterized queries
    - XPath Injection : no use of XPath
    - LDAP Injection : no use of LDAP queries
    - Command Injection : no use of command line in php code
- Path Traversal : image auto resizing and cropping validates MIME type of the file being requested, and is limited to user content images directory

- Cross Site Scripting (XSS) : Data collected from user is stored, and displayed, using appropriate escaping function
- Integer Overflows : for each numerical input, length and type are validated
- XML External Entities : No XML resources loaded from outside system

Netkin office and equipment security

- Local network protected by WatchGuard Firebox M200 appliance ;
- BitDefender GravityZone antivirus (with centralized management system and automatic updates, users cannot deactivate, uninstall or set up the antivirus), with patch management extension ;
- Intrusion and fire detection by Securitas Direct / Verisure (APSAD R31 P3 certification) ;
- Video-surveillance of all the places where our employees pass through our premises, with retention of the videos for 30 days ;
- Our employees' email accounts are Gmail Enterprise accounts with 2FA enabled ;
- No wifi access allowed to the local network.

Security policy for Netkin staff and event subcontractors

- All employees are on full-time contracts and have signed a specific non-disclosure agreement (NDA) covering all internal and customer data.
- Only required employees are allowed to access the data and they are not allowed to keep a copy of the data. All employees have signed this as part of their NDA.
- Employees are not allowed to keep a copy of customer data outside of the customer's instance. Any temporary copy (received by any means, including email) or extract from the client instance must be deleted immediately after use. Any extraction of data must be performed by the customer using their administrative access to the platform. We do not perform data extraction on behalf of our clients.
- If an event requires the intervention of a subcontractor (freelance in particular), this is not done without the agreement of our client, and we sign a data subcontract with the subcontractor.

Security policy for technical staff

- Development on a local server in our offices, test and staging servers at OVH with automatic antivirus analysis, automated and human functional tests, and Acunetix scan performed by the CSO on each release candidate before its publication.

- The production instances are then automatically deployed by our instance manager, which is only accessible from our technical VPN (OpenVPN Access Cluster managed by us on dedicated OVH servers, with individual accounts, password rotation every night, daily mandatory 2FA OTP, and audit of all connections in OpenVPN)
- This manager installs the source code, database, mailboxes, SSL certificates and sends administrative access to the client, who can then grant access to other administrators if needed.
- Developers do not have access to the database server
- Developers do not have access to the source code of a production instance, unless specifically authorized by management and/or the customer (only upon written request, telephone requests are not allowed).
    - If a temporary access is granted, it is only accessible from our technical VPN (OpenVPN Access Cluster managed by us on dedicated OVH servers, with individual accounts, password rotation every night, daily mandatory 2FA OTP, and audit of all connections in OpenVPN)
- Access to technical logs (apache, Imunify360, etc.) is only possible for the CTO or deputy CTO, or exceptionally to another developer, on a temporary basis.

Business continuity policy (backup and recovery of data, time to restore)

Every instance is backuped once a day on a secure off-site OVH datacenter. Backups are retained daily for one week, and then weekly or monthly, until data destruction (see bellow).

- Daily automated database and user files backup, crypted with AES-256-CBC, to secured storage server. **RPO** is thereby of 24 hours.
- Monitoring of automated backup
- Data recovery and business continuity in case of server failure (**RTO**) :
    - **Registration website (used before the event) :** 4 hours
    - **Event live application (user during the event, amongst others for interactivity sessions)** : Load balancing is performed at the client level with the following principle : each client looks for the fastest responding server amongst 4, which are located in 2 distinct datacenters (Roubaix in France, and Strasbourg in France). Each server contains the same replica of data, and is synced realtime with the others, with full network failure tolerance and recovery. With the architecture, even in the very unlikely event of failure of 3 servers at the same time, the app will still be fully operational.

We commit to a 99,95% SLA on platform general availability. This exclude any misconfiguration made by the client when self-administering the platform, as well as misconfigured or obsolete clients that might not be able to access or display the registration website or event app.

Data conservation policy

By default, 1 year after the deployment of an event instance (site + app), the participating data is automatically deleted, after 3 email alerts to the main site administrator.

After 3 years, all data is automatically destroyed, including backups. If you wish, you can ask us to reduce or increase this period, in compliance with the legislation in force.

Any questions ?

For any further information, please do not hesitate to contact us at the following email address: *support@netkin.fr*